The Defense Biometrics Identification System

By Michele Buisch

Because of the current problem with identity theft, verifying identification cannot be taken too lightly, especially when someone is trying to gain access to a military installation.

Such a security breach can mean life or death consequences. In December 2004, 22 people in an Army dining hall were killed, and many more were wounded when a suicide bomber wearing an Iraqi security forces uniform made his way onto the base in Mosul, Iraq, according to published reports.

A military guard checks the identification of a visitor using the Defense Biometric Identification System (DBIDS) wireless handheld device.

To secure Department of Defense (DoD) locations throughout the world, the Defense Manpower Data Center (DMDC) has developed an identification system that uses barcodes and biometrics to identify cardholders. The Defense Biometric Identification System (DBIDS) is a DoD identity authentication and force protection tool that is fully operational in military locations around the world. Commander, Fleet Activities Yokosuka (CFAY), Japan, is the latest military installation to pilot the DBIDS program and the first U.S. Navy installation to do so.

As DoD's largest physical access control system, DBIDS uses fingerprints and, in some cases, hand geometry to accurately identify personnel entering military installations. This system is more secure and quicker for personnel entering a military installation than flashing an identification (ID) card at a guard who then must compare the picture on the ID card to the cardholder. In addition to validating identity credentials, DBIDS also verifies authorizations and assigns access privileges based on identity, affiliation and the current threat level. Unlike the "flash pass" method, DBIDS reveals phony or expired ID cards and anyone unauthorized to access military installations. DBIDS identifies individuals who are wanted, barred from the installation or have other law enforcement alerts.

Active duty personnel, family members, DoD contractors and retirees are registered in DBIDS using their Common Access Card (CAC) or any DoD-issued identification credential. For people who do not have DoD credentials, but require access to the base, DBIDS provides a way to identify these individuals. Once these individuals, including foreign national employees, guests, frequent visitors (such as taxi or delivery drivers), children of DoD employees and U.S. Embassy personnel, are entered into the system, they are given a DBIDS identification card. DoD identification cardholders use the card they have already been issued, such as the CAC.

Originally called the Biometrics Identification System (BIDS), BIDS was created at the request of U.S. Forces Korea in 1998 as a force protection system in recognition of the tenuous truce between North and South Korea.

Since a peace treaty was never signed, and the peninsula is under an armistice, there are times of heightened concern that require an enhanced security posture. In response, by early 2000, BIDS was deployed to numerous locations in Korea. Then the Sept. 11, 2001, terrorist attacks on the United States resulted in full implementation at all military installations in Korea with scanning at all gates 24 hours a day.

In addition to enhancing force protection in Korea, DBIDS has assisted in the investigation of several crimes. In one case, the DBIDS audit capability helped law enforcement officials identify two suspects in the murder of an active duty Army Soldier based on the times the suspects entered the base. Once identified, one of the suspects admitted to committing the murder.

At another Korean installation, DBIDS identified an individual who had stolen a vehicle and a CAC inside the vehicle. Two days after the vehicle and the CAC were reported stolen the information was entered into the system. When the individual attempted to enter the installation, DBIDS alerted the guard to the stolen CAC and the person was apprehended.

At CFAY, two barred individuals and two wanted individuals were identified trying to enter the installation shortly after the guards began using DBIDS. In addition, the audit capability was used to investigate the beating of a Sailor off base.

Although DBIDS has proved successful in Korea and at other military installations, Patrick J. McGee, manager for Asia Operations, DMDC, said DMDC still faces the challenge of demonstrating the system's benefits and ease of use. "Confidence in the system is paramount, and while DBIDS does prove itself quickly once put into action, overcoming the resistance to change paradigm is sometimes a difficult thing," McGee said. "Once put into use, however, users can't believe they lived without it."

The system works like this: The guard scans the card's barcode and/or the individual's fingerprints *(depending on the Force Protection Condition (FPCON) level and installation policy)* using a wireless, handheld device. Then the guard reviews screen displays to verify that the ID card is an authorized DoD credential

that is not expired, lost or stolen. It also verifies the individual's identity and that he or she is not wanted, barred or suspended from entering the installation, and has access to the installation under the Force Protection Condition.

If a restriction has been placed on the individual, the screen display will tell the guard how to proceed. "DBIDS virtually eliminates the threat of unauthorized persons gaining access; stopping them at the front door so to speak," McGee said. "And these operations not only act as a physical protection measure but also as a deterrent."

The screen displays include color photo, identity information, color-coded message screens, audible sounds to quickly and easily alert the guard of the individual's status and a variety of administrator capabilities. In addition, the text on the screens is multilingual. "All this occurs in a matter of two to three seconds of the scan, less time than it takes the guard to visually validate an ID card," McGee said.

The scalable system can cover a building, installation or entire theater of operations. The majority of DBIDS sites, including CFAY, use fingerprint scans when the FPCON or installation policy dictates that additional checks are required. However, DBIDS Kuwait uses hand geometry because of the difficulty encountered in trying to capture usable fingerprints from laborers.

At CFAY, DBIDS equipment was deployed in 2004 with the opening of a registration center. In April, gate access and the Visitor Control Center were installed. Nearly 32,000 people are registered at CFAY in DBIDS and approximately 22 percent are DBIDS cardholders. The remainder are DoD identification cardholders, according to McGee.

Fully operational DBIDS installations include: U.S. Armed Forces Europe; U.S. Armed Force Korea; Fort Hood, Texas; Fort Polk, La.; Monterey Peninsula, Calif.; and U.S. Joint Task Force, Southwest Asia (Kuwait and Qatar).

DBIDS expansion is an ongoing process throughout many areas of the DoD. This expansion has led to the creation of the new Identity Authentication Office within DMDC, which is dedicated to managing DBIDS. In addition to working on improved versions of the system, the office is investigating linking to other government identity authentication systems to share data and digital fingerprints using CAC chips for authentication.

New DBIDS deployments are underway at Yokota Air Base in Japan and other areas in Southwest Asia, according to McGee.

For more information about DBIDS, please visit the DBIDS Web site at https://www.dmdc.osd.mil/dbids/.

Michele Buisch is a contractor supporting the Department of the Navy Chief Information Officer. CHIPS

Implementation of PKI Authentication for DADMS

The use of the Public Key Infrastructure (PKI) and the Common Access Card (CAC) for accessing the Department of the Navy Applications and Database Management System (DADMS) became mandatory Sept. 6, 2005, according to a coordinated naval message: AL NAVADMIN (UC) R 012042Z SEP 05 issued by the Department of the Navy Chief Information Officer (DON CIO) and the Assistant Chief of Naval Operations for Information Technology (ACNO-IT).

This action is being taken to provide additional assurance that only personnel authorized by the current DADMS access control process have access to the network and application information contained in DADMS.

DADMS users must either have a valid PKI software certification (softcert) installed on their system or use a CAC reader and software to provide the authentication.

DADMS users are advised that PKI softcerts have an expiration date at which time the softcert will become invalid. Softcerts are no longer being issued. Once the softcert expires users will be required to use their CAC for authentication.

Navy Marine Corps Intranet (NMCI) desktop computers or laptops are provided with a CAC reader and ActivCard Gold software required for authentication purposes. In addition to the CAC and ActivCard Gold software, users must enter their individual personal identification number (PIN) code which they created when their CAC was issued.

Users accessing DADMS from non-NMCI computers must have a CAC reader attached to their computer as a peripheral and have the ActivCard Gold PKI Common Access Card software installed to provide the authentication.

PKI authentication is in addition to the user identification (ID) and password currently required to log onto DADMS. PKI authentication does not change the current method of obtaining access to DADMS. Any DADMS user ID and password problems should still be reported to the DADMS help desk. CAC problems are to be reported to command CAC issuing activities since the DADMS help desk cannot assist with CAC problems.

Use of the CAC to access DADMS can be tested immediately and is encouraged to ensure CAC problems have been addressed.

For additional information contact the ACNO-IT at (703) 604-7813. CHIPS